

Biztonság és védelem az informatikában

9. gyakorlati feladat

Készítette: Baranyi Gábor
CRC7FC

2021.04.15.

Titkosítási gyakorlatok

1.feladat számolása:

$$1\,920 * 1\,080 = 2\,073\,600$$

$$2\,073\,600 * 3 = 6\,220\,800$$

$$6\,220\,800 * 3 = 18\,662\,400$$

$$18\,662\,400 / 8 = 2\,332\,800$$

válasz:

2 332 800 bájt információ fér el egy képen

2.feladat számolása:

$$2\,332\,800 / 60 = 38\,880$$

$$38\,880 / 30 = 1\,296$$

Tehát 1 296 A/4-es lapot tesz ki.

Alkalmazás mely képes titkosítani illetve azt visszfejteni:

jp hide & seek

Az adatrejtett kép a következőket tartalmazza:

- „William Shakespeare teljes művei”
 - 37 darab, 154 szonett
 - 124 788 sornyi szöveg
 - 10 004 560 szó
- 1080p asztali háttér (1920x1080) Elrejthetünk:
 - 1 555 200 bájt

Az eredeti kép:



Adatrejtés utáni kép:



Titkosítás 1:

Eredeti mondat:

„amit hárman tudnak, már nem titok”

Caesar-rejtjel:

cokú jcstocó úúéócm, ocst ógo úkúőm

Kulcsszavas behelyettesítés:

kulcsszó:SOMA

skgt foqksi tublsi, koq ldk tgti

XOR-kódolás

bitminta: 01001100

-!%8l\$>!-"l89("-`l!>l")!l8%8#'

Titkosítás 2:

Eredeti szöveg:

„Kertészkedem mélán, nyugodtan,

Gyümölcsfáim közt bíbelek;

Hozzám a tiszta kék magasból

Egyes daruszó tévelyeg;

Felém a kert gyepűin által

Egy gerlice bűgása hat:

Magános gerle a szomszédban -

S ifjú nő, szemfödél alatt.

Kevés ember jó látogatni,
Az is csak elmegy hidegen:
Látszik, hogy a halott szegény volt,
Szegény s amellet idegen.
Rokonait, ha van rokonja,
Elnyelte széles e világ;
Nem nyit be hozzá enyhe részvét,
Legföljebb... a kíváncsiság.”

írásjelek, ékezetek nélkül:

kerteszkedemmelannyugodtangyumolcsfaimkoztbibelekhozzamatisztakekmaga
sbolegyesdaruszotevelyeg;felemakertgyepuinaltaleygerlicebugasahatmaganos
gerleaszomszedbansifjunoszemfodelalattkevesemberjolatogatniaziscsakelmegy
hidegenlatszikhogyahalottszegenyvoltSzegenysamellettidegen.rokonaithavanro
konjaelnyelteszelesevilagnemnyitbehozzaenyhereszvetlegfoljebbakivancsisag

Caesar kódolt:

pjwyxepjijrrjqfssdzltiyfslldzrtqhxfkfnrpteyngjqjpmteefrfynxeyfpjprflfxgtqjldjxif
wzxetyjajqdjljkjrpfjwyldjuznsfyyfjldljwqnhjgzlfxmfyrflfstxljwqjfxetrxejigfsxnk
ozstxejrktijqfyyppajxjrgjwotqfytlfysnfexhxfpjqrjldmnijlsqfyxenpmtldmfqtyyx
ejljsdatqyxejljsdxfrjqjyynijlswtptsfnymfafswtptsofjqsdjqyxejqjxjanqflsjsrdnygj
mteefjsdmjwjxeajyqjltqojggfpnafshxnxfl

Források:

https://en.wikipedia.org/wiki/XOR_cipher

<https://hu.wikipedia.org/wiki/Caesar-rejtjel>